

**DEPARTMENT OF VETERANS AFFAIRS
INFORMATION SECURITY RULES OF BEHAVIOR
FOR NON-ORGANIZATIONAL USERS**

1. COVERAGE

a. Department of Veterans Affairs (VA) Information Security Rules of Behavior (ROB) for Non-Organizational Users provides the specific responsibilities and expected behavior for non-organizational users of VA systems and VA information as required by 38 U.S.C. § 5723(f)(5), OMB Circular A-130, Appendix I, §§ 4(h)(6-7) and VA Handbook 6500, *Managing Information Security Risk: VA Information Security Program*.

b. *Organizational users* are identified as VA employees, contractors, researchers, students, volunteers, and representatives of Federal, state, local or tribal agencies not representing a Veteran or claimant.

c. *Non-organizational users* are identified as all information system users other than VA users explicitly categorized as organizational users. These include individuals with a Veteran/claimant power of attorney. Change Management Agents at the local facility are responsible for on-boarding power of attorney/private attorneys.

d. VA information is information under the control of VA or stored on a VA information system. This includes both VA sensitive and non-sensitive information. Information properly disclosed by VA to a non-organizational user (e.g., contents of a Veteran's claims file for purposes of representing a Veteran or claimant) is no longer VA information and its security and confidentiality is the responsibility of the recipient.

e. The VA ROB for Non-Organizational Users does not supersede any policies of VA facilities or other agency components that provide higher levels of protection to VA's information or information systems. The ROB simply provides the minimum standards with which individual users must comply, and VA facilities and other agency components may issue standards for protection that exceed the ROB. In addition, authorized users are required to go beyond stated rules using due diligence and the highest ethical standards.

2. COMPLIANCE

a. Non-compliance with the VA ROB for Non-Organizational Users may be cause for suspension or removal of access to VA information or information systems. Such a suspension would not prevent the authorized disclosure of records to an individual; however, it may prevent disclosure through a particular method, e.g., by suspending of access through a VA information system. Depending on the severity of the violation and management discretion, consequences may include restricting access or suspension of access privileges. Theft, conversion, or unauthorized access, disposal, or destruction of Federal property or disclosure of information may result in criminal sanctions.

Initials_____

Date_____

b. Accessing, uploading, downloading, changing, circumventing, or deleting of information on VA systems without authorization; modifying VA systems, denying or granting access to VA systems without authorization; using VA resources for unauthorized purpose on VA systems; or otherwise misusing VA systems or resources is strictly prohibited and may result in criminal sanctions.

c. The VA ROB for Non-Organizational Users does not create any other right or benefit, substantive or procedural, enforceable by law by a party in litigation with the U.S. Government.

3. ACKNOWLEDGEMENT

a. The VA ROB for Non-Organizational Users must be signed before access is provided to VA information or information systems and annually thereafter by non-organizational users of VA information or information systems. This signature indicates agreement to adhere to the ROB. Refusal to sign the ROB will result in denial of access to VA information or information systems.

b. The VA ROB for Non-Organizational Users may be signed in hard copy or electronically. If signed using the hard copy method, the user should initial and date each page and provide the information requested under Acknowledgement and Acceptance.

4. INFORMATION SECURITY RULES of BEHAVIOR

Access and Use of VA Information Systems

I Will:

- Comply with all federal and VA information security, privacy, and records management policies. SOURCE: VA Handbook 6500 Control PM-1
- Have NO expectation of privacy in my activities while accessing or using VA information systems, as I understand that all activity is logged for security purposes. SOURCE: VA Handbook 6500 Control AC-8
- Follow established procedures for requesting access to any VA information system and for notifying VA when the access is no longer needed. SOURCE: VA Handbook 6500 Control AC-2
- Only use my access to VA computer systems and/or records for officially authorized purposes. SOURCE: VA Handbook 6500 Control AC-6
- Only use VA-approved solutions, software, or services for connecting non-VA-owned systems to VA's network either remotely or directly. SOURCE: VA Handbook 6500 Control AC-20, AC-17

I Will Not:

- Attempt to probe computer systems to exploit system controls or to obtain unauthorized access to VA sensitive data. SOURCE: VA Handbook 6500 Control AC-6
- Use personally-owned equipment on-site at a VA facility to directly connect to the VA network, or connect remotely to the VA network unless approved prior to use

Initials_____

Date_____

(i.e., approval from VA ISO or Change Management Agent). SOURCE: VA Handbook 6500 Control AC-20

Protection of Computing Resources

I Will:

- Protect Government Furnished Equipment (GFE) from theft, loss, destruction, misuse, and threats. SOURCE: VA Handbook 6500 Control AC-17
- Follow VA policies and procedures for handling Federal Government IT equipment and sign for items provided to me for my exclusive use and return them when no longer required for VA activities. SOURCE: VA Handbook 6500 Control CM-8(4)

I Will Not:

- Swap or surrender VA hard drives or other storage devices to anyone other than an authorized OI&T employee. SOURCE: VA Handbook 6500 Control MP-4
- Attempt to override, circumvent, alter, or disable operational, technical, or management security configuration controls unless expressly directed to do so by authorized VA staff. SOURCE: VA Handbook 6500 Control CM-3

Electronic Data Protection

I Will:

- If authorized to directly connect to a VA system, only use virus protection software, anti-spyware, and firewall/intrusion detection software authorized by VA. SOURCE: VA Handbook 6500 Control SI-3

I Will Not:

- Download or install prohibited software from the Internet, or other publicly available sources, offered as free trials, shareware, or other unlicensed software to a VA-owned system. SOURCE: VA Handbook 6500 Control CM-11
- Disable or degrade software programs used by VA that install security software updates to VA computer equipment, to computer equipment used to connect to VA information systems, or used to create, store, or use VA information. SOURCE: VA Handbook 6500 Control CM-10

Remote Access

I Will:

- Protect information about remote access mechanisms from unauthorized use and disclosure. SOURCE: VA Handbook 6500 Control AC-17

I Will Not:

- Access non-public VA information systems from publicly-available IT computers, such as remotely connecting to the internal VA network from computers in a public library. SOURCE: VA Handbook 6500 Control AC-17

- Access any VA information system from any foreign country unless approved by a VA ISO, local CIO, and Information System Owner. SOURCE: VA Handbook 6500 Control AC-17

User Accountability

I Will:

- Complete mandatory security and privacy awareness training within designated time frames. SOURCE: VA Handbook 6500 Control AT-3
- Complete any additional role-based security training required based on my role and responsibilities. SOURCE: VA Handbook 6500 Control AT-3
- I understand that authorized VA personnel may review my conduct or actions concerning VA information and information systems, and take appropriate action. SOURCE: VA Handbook 6500 Control AU-1
- If applicable, have my GFE scanned and serviced by VA authorized personnel. This may require me to return it promptly to a VA facility upon request. SOURCE: VA Handbook 6500 Control MA-2
- Permit only those authorized by OI&T to perform maintenance on GFE or VA IT components, including installation or removal of hardware or software. SOURCE: VA Handbook 6500 Control MA-5
- Sign specific or unique ROB as required for access or use of specific VA systems or non-VA systems. SOURCE: VA Handbook 6500 Control PL-4

Sensitive Information

I Will Not:

- Disclose information relating to the diagnosis or treatment of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia by VA without appropriate legal authority. Unauthorized disclosure of this information may have a serious adverse effect on agency operations, agency assets, or individuals, and includes criminal penalties. SOURCE: VA Handbook 6500 Control IP-1, 38 U.S.C. § 7332

Identification and Authentication

I Will:

- Use passwords that meet the VA minimum requirements. SOURCE: VA Handbook 6500 Control IA-5(1)
- Protect my passwords; verify codes, tokens, and credentials from unauthorized use and disclosure. SOURCE: VA Handbook 6500 Control IA-5(h)

I Will Not:

- Store my VA passwords or verify codes in any file on any IT system, unless that file has been encrypted using FIPS 140-2 (or its successor) validated encryption, and I am the only person who can decrypt the file. SOURCE: VA Handbook 6500 Control IA-5

- Hardcode credentials into scripts or programs. SOURCE: VA Handbook 6500 Control IA-5(1)(c)
- Divulge a personal username, password, access code, verify code, or other access credential to anyone. SOURCE: VA Handbook 6500 Control AC-17

Incident Reporting

I Will:

- Report suspected or identified information security incidents including anti-virus, antispyware, firewall or intrusion detection software errors, or significant alert messages (security and privacy) on VA information systems to a VA ISO, local CIO, and Information System Owner immediately upon suspicion. SOURCE: VA Handbook 6500 Control IR-6

5. ACKNOWLEDGEMENT AND ACCEPTANCE

- I acknowledge that I have received a copy of the VA Information Security Rules of Behavior for Non-Organizational Users.
- I understand, accept, and agree to comply with all terms and conditions of the VA Information Security Rules of Behavior for Non-Organizational Users.

Print or type your full name

Signature

Date

Office Phone _____

Position Title _____